Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the subject application.

Listing of Claims:

What is claimed is:

1. (Currently Amended): An integrated firewall/VPN system, comprising:

at least one wide area network (WAN);

at least one local area network (LAN); and

an integrated firewall/VPN chipset ~~adapted~~ configured to send and receive data packets between said WAN and said LAN, said chipset comprising:

a firewall ~~portion and~~ comprising ~~to provide access control between said WAN and said LAN and a VPN portion adapted to provide security functions for data between said LAN and said WAN; said firewall including firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with said access control~~ a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching and a fourth layer including a session match engine configured to store a TCP/UDP connection setup and to forward the setup progress to a central processing unit (CPU) for tracking; and

a VPN ~~potion including VPN hardware and software portions wherein at least VPN hardware portion is adapted~~ configured to provide ~~iterative functions associated with said~~ security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets.

2. (Currently amended): A system as claimed in claim 1, wherein said chipset further comprises a router adapted to route data between said WAN ~~LAN~~ and said LAN.

3. (Currently amended): A system as claimed in claim 1, wherein said firewall ~~hardware portion comprising circuitry~~ is configured to provide static and/or dynamic data packet filtering.

4. (Currently amended): A system as claimed in claim 3, wherein said ~~circuitry includes a~~ header match packet filtering ~~circuit~~ engine is configured to provide pattern matching in selected headers of said data and their combination from L2, L3 and L4 headers.

5. (Currently Amended): A system as claimed in claim 1, wherein said chipset is further ~~adapted~~ configured to analyze access control functions based on preselected bytes of said data packets.

6. (Original): A system as claimed in claim 5, wherein said preselected bytes comprise the first 144 bytes of said data packet.

7. (Cancelled):

8. (Currently Amended): A system as claimed in claim 1, wherein said firewall further includes access control functions ~~comprise~~ comprising user-defined access control protocols.

9. (Currently amended): A firewall/VPN integrated circuit (IC), comprising:

a router core ~~adapted~~ configured to interface between at least one untrusted network and at least one trusted network to send and receive data packets between said untrusted and said trusted networks;

a firewall system ~~adapted to provide access control between said untrusted and said trusted networks, and comprising firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with said access control~~, comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match

packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching and a fourth layer including a session match engine configured to store a TCP/UDP connection setup and to forward the setup progress to a central processing unit (CPU) for tracking; and

a VPN engine ~~adapted~~ configured to provide security functions for data between said at least one untrusted and said at least one trusted network~~s~~, ~~and comprising VPN hardware and software wherein at least said VPN hardware portion is adapted to provide iterative functions associated with said security functions~~, wherein said security functions comprise encryption, decryption, encapsulation, and decapsulation of said data packets.

10. (Currently amended): An IC ~~system~~ as claimed in claim 9, wherein said firewall ~~hardware portion comprising circuitry~~ system is configured to provide static and/or dynamic data packet filtering.

11. (Currently amended): An IC as claimed in claim 10, ~~wherein said circuitry includes a~~ wherein said header match packet filtering circuit is configured to provide pattern matching in selected headers of said data and their combination from L2, L3 and L4 headers.

12. (Currently Amended): An IC as claimed in claim 9, wherein said firewall system is further ~~adapted~~ configured to analyze access control functions based on preselected bytes of said data packets.

13. (Original): An IC as claimed in claim 12, wherein said preselected bytes comprise the first 144 bytes of said data packet.

14. (Cancelled):

15. (Currently amended): An IC ~~A system~~ as claimed in claim 9, wherein said firewall system further includes access control functions ~~comprise~~ comprising user-defined access

control protocols.

16. (Currently Amended): A method of providing firewall access control functions, comprising the steps of:

defining one or more access control protocols;

receiving a data packet;

selecting a certain number of bytes of said data packet;

processing said selected bytes using said access control protocols~~.~~ via a firewall system comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of said data packet, a third layer including at least one application proxy configured to provide additional pattern matching and a fourth layer including a session match engine configured to store a TCP/UDP connection setup and to forward the setup progress to a central processing unit (CPU) for tracking.

17. (Cancelled)